ABSTRACT

A method and system that protect selected system and other files, by preventing changes to those files. In an asynchronous alternative, the change is prevented by copying back the original file when a protected file is changed, as known via an asynchronous notification. In an alternative, synchronous embodiment, the change to the file is prevented from occurring. In the asynchronous notification alternative, a directory change notification notifies a file protection service whenever a file that has possibly changed is closed, providing the file identity as part of the notification. The file protection service determines from the file identify whether the file has been deemed protected. If protected, the file protection service prevents any actual change by verifying whether the protected file changed, such as by analyzing the file's contents against known valid contents. If not valid, the file protection service restores a saved copy that is itself verified. In the asynchronous alternative, changes are saved via a copy-on-write, and those changes are saved if valid or discarded if not, transparent to the application. Exceptions are provided to enable certain critical protected files to be replaced when necessary.